IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 June 2023, accepted 2 July 2023, date of publication 7 July 2023, date of current version 19 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3293063

TOPICAL REVIEW

Uncovering the Cloak: A Systematic Review of Techniques Used to Conceal Phishing Websites

WENHAO LI, (Graduate Student Member, IEEE), SELVAKUMAR MANICKAM, SHAMS UL ARFEEN LAGHARI, AND YUNG-WEY CHONG

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, George Town, Penang 11800, Malaysia

Corresponding authors: Selvakumar Manickam (selva@usm.my) and Shams Ul Arfeen Laghari (shamsularfeen@nav6.usm.my)

ABSTRACT Phishing represents a cybersecurity attack strategy commonly employed by cybercriminals to unlawfully acquire sensitive user information, including passwords, account details, credit card data, and other personally identifiable information. Phishing websites bear a striking resemblance to their legitimate counterparts, thus rendering them inconspicuous and challenging for an unsuspecting user to identify. Criminals and phishing experts frequently leverage cloaking mechanisms to evade detection software and web crawlers. This paper provides a comprehensive systematic review of primary studies conducted between 2012 and 2022 on using cloaking techniques to evade detection by anti-phishing entities based on data extracted from Scopus, Web of Science, and Google Scholar. Different server-side and client-side detection strategies, phishing techniques and cloaking mechanisms, toolkits, blacklists, phishing or anti-phishing ecosystems, and other such concepts have been taken as thematic outputs of the study and have been discussed in detail. This systematic literature review (SLR) is one of the first reviews to be conducted for analyzing the current cloaking or evasion techniques used by phishers, and the limitations of the study have been outlined as well.

INDEX TERMS Anti-phishing ecosystem, cloaking techniques, evasion techniques, phishing toolkit, phishing blacklist.

I. INTRODUCTION

Phishing is a cybercrime and online theft strategy criminals use to steal a person's personal information and credentials [1]. It allows the attacker to access a user's private information using fake websites similar to the original ones and can be troublesome to recognize [2], [3], leading to successful attacks on naive users. There are many channels such as social media, email and text message available for use by criminals to conduct phishing attacks. One of the most frequently used methods for phishing is the creation of phishing websites that mock official real websites. Attackers send links to users via the aforementioned channels in an attempt to lure the users to visit [4].

With a notion rooted deep in history, phishing emerged in the mid-90s, evolving from the age-old practice of phone phreaking - an era marked by the manipulation of telecommunication systems for unauthorized activities. This laid the foundation for the deceptive strategies that would later become the cornerstone of phishing. The term "phishing" itself, coined in 1996, stemmed from hackers pilfering America Online (AOL) accounts and passwords. This metaphorical term, drawing parallels with "fishing", symbolizes the hackers' strategy of casting 'bait' to 'catch' passwords and financial data from the internet's vast 'ocean' of users. These hackers commonly targeted AOL's extensive dial-up service, duping users with messages disguised as official AOL correspondences, thereby acquiring their login details and credit card information [5]. Moving into the 2000s, the art of phishing underwent a transformation, with malefactors turning to phishing websites as their weapon of choice. The proliferation of online banking made financial institutions an attractive target, with deceptive websites mimicking genuine bank portals being established to trick users into surrendering their login details. The complexity and range of phishing attacks

The associate editor coordinating the review of this manuscript and approving it for publication was S. K. Hafizul Islam.

have only amplified over time. Recent advancements in technologies such as 5G and the Internet of Things (IoT) have not only resulted in an increased availability of devices [6] but are also projected to continue this upward trend in the foreseeable future [6]. Consequently, individuals are increasingly leveraging online transaction facilities for a wide array of activities including bill payments, money transfers, and online shopping. Phishers have used this trend to their benefit and often inject phishing content into vulnerable websites or pose as brands by using fake websites with designs similar to the originals to steal credentials and gain access to the financial accounts of the users [7], [8]. Phishing as one of the cybercrimes not only targets individuals but also organizations and government departments leading to potential data breaches, reputation damages and financial losses [9].

More specifically, phishing can be classified into two types: general phishing and spear-phishing. The former involves a relatively large-scale attack, while the latter aims at a certain group of people or an organization with highly customized information [10]. Advanced persistent threat (APT) 37, also known as Ricochet Chollima, is a well-known APT group. In a report by the US security company FireEye, it was disclosed that APT 37 used a bank letter as a spear-phishing lure to target a board member of a Middle Eastern company with a crafted attachment, exploiting the CVE-2017-0199 vulnerability in May 2017 [11]. On May 7, 2021, the largest oil pipeline company, Colonial Pipeline, suffered a ransomware attack that led to a six-day shutdown of its operations, thereby posing a threat to US national security. The company had to pay the attacker using bitcoins, although the Department of Justice of the United States later claimed that they seized a partial amount of the bitcoins. This was the largest known attack on the oil infrastructure in the history of the United States, and it is believed that spear-phishing was used as the entry point for the attackers [12].

Even though phishing might seem trivial, it is a very effective tactic for cybercriminals as it can bypass a variety of security measures that organizations put in place, including Web Application Firewall (WAF), Intrusion P revention System (IPS), Intrusion Detection System (IDS), honeypots, antivirus software, and firewalls at different application, system, and network levels. Finding and exploiting vulnerabilities on systems and servers typically require enormous amounts of time; this is where phishing becomes the most efficient method for a cybercriminal. Through phishing, the attacker can sometimes obtain direct access to both critical information and intranet without having to find and exploit vulnerabilities, bypassing security policies. In summary, phishing is low-cost yet it promises unexpected returns, making it a prime motivation for attackers.

The escalating prevalence of phishing attacks in recent years has resulted in substantial financial ramifications. This troubling trend was highlighted in a report disseminated by the Anti-Phishing Working Group (APWG) in December 2022, which showed a staggering five-fold increase in phishing incidents during Q3 2022 compared to Q4 2016,

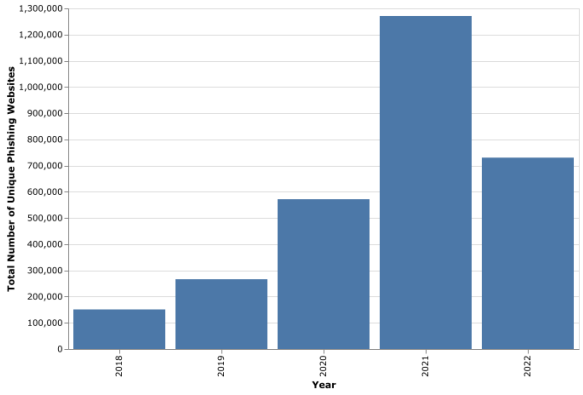

FIGURE 1. Total Number of Unique Phishing Websites Detected in 3rd Quarter from 2018-2022.

culminating in an alarming 1,270,883 recorded attacks in just the third quarter of 2022 alone [13]. In addition, Fig. 1 elucidates a consistent upward trend in the detection of phishing websites from Q3 2018 to 2022 [13], with 2021 witnessing the most dramatic surge. This spike is potentially attributable to the COVID-19 pandemic, which significantly increased internet usage for professional and personal purposes. The escalating trend of phishing attacks has led to significant financial implications. A 2022 cybercrime report from AAG IT Company highlighted the severity of the financial damage inflicted by these attacks, revealing an astonishing $44.2 million was siphoned off through phishing in 2021 alone, averaging $136 per assault [14]. These figures underscore the urgent necessity to counter phishing attacks effectively.

An array of detection software and technologies is deployed to identify phishing websites and malicious content across the World Wide Web (WWW), thereby safeguarding users from cyber threats. Certain detection schemas capitalize on the lexical features of URLs to identify phishing websites [15], [16], [17], while others rely on website content, pinpointing potential phishing threats through visual and/or textual resemblances [18], [19], [20]. Nonetheless, these mechanisms harbor salient limitations. Primarily, they require rule and/or feature extraction from datasets for website classification, thereby faltering in the face of unknown features. Furthermore, these methods exhibit high latency in detection and incur significant costs when tackling large-scale phishing operations. Complicating matters further, phishing content has evolved over time, exploiting the vulnerabilities of detection systems [21], [22], [23], [24]. In addition, phishers employ evasion and cloaking techniques to remain concealed from current detection mechanisms, with crawlers deployed to gather information from potential phishing websites, revealing phishing content exclusively to entities deemed actual human users [25], [26], [27]. Consequently, it becomes crucial to scrutinize the various cloaking mechanisms employed by phishers, alongside the detection systems designed to identify such content.

Several studies have been conducted in recent years addressing the issue of phishing. Jain and Gupta [28] conducted an SLR on phishing attacks, which studied the lifecycle of an attack, its history, attack motivation, various distribution methods, protection mechanisms, challenges faced by developers, and open issues. Sharma et al. [29] reviewed the various anti-phishing techniques and defense mechanisms. In another review, the researchers examine AI-based detection mechanisms of phishing websites [30]. However, in these recent reviews, there is a lack of focus on the Anti-phishing Ecosystem, Phishing Blacklists, and toolkits. This study aims to provide a more comprehensive SLR while focusing on the research characteristics, the phishing ecosystem, and the various evasion/cloaking techniques missing in the recent reviews mentioned above. It is also used as a guide for developing the prevention of phishing attacks especially for phishing websites, through more advanced techniques. The contributions of this paper are as follows:

1) We adopted a SLR approach to analyze the relevant studies and selected a total of 30 articles based on several criteria to support this research.
2) We identified the research characterstics of present studies and extracted the most important thematic findings to understand the state-of-art topics in this domain.
3) We identified the reported cloaking or evasion mechanisms employed in phishing websites and the strategies and tools used to detect from the selected studies and this is one of the first reviews to be conducted for analyzing the current cloaking or evasion techniques used by phishers.

This study is organized into five sections. (1) Section II presents the fundamental background and essential concepts of the study by reviewing the related literature. (2) Section III offers a thorough evaluation of the obtained literature related to this review. (3) Section IV highlights the characteristics of the current research and thematic findings. (4) Section V assesses the state-of-the-art evasion/cloaking techniques employed by phishing websites. This includes the technical methods used to cloak and the related detection strategies against these cloaks. (5) Finally, Section VI provides the discussion and conclusions.

II. REVIEW OF LITERATURE

A. PHISHING TOOLKIT

A phishing toolkit can be defined as software tools designed to assist immature individuals in developing and launching a phishing attack, which simplifies the creation of phishing websites [31]. It can also be defined as a set of tools to deploy a phishing website on a web server [3], [32]. Phishing toolkits may be designed by the creators for personal use or can be bought and sold on the Internet as a part of the cybercrime-as-a-service economy [33]. The basis on which kit creators focus in the design is the ease of use and perceived security, i.e., the ability to evade the detections of anti-phishing systems [2]. The tools in a phishing kit may lower the chances of being captured as a phishing website and allow criminals to become successful phishers with minimal technical knowledge and prowess. The essential components that are present in a phishing kit may include a template of a website that is to be impersonated, some server-side code that is used for capturing and sending the data that is submitted on the website to the phisher, and sometimes may also include some optional code that can be used for filtering out unwanted traffic or implementation of countermeasures for anti-phishing systems [3]. Various phishing toolkits are available on the Internet. Conventional toolkits, such as Zphisher [34], KingPhisher [35], sptoolkit [36], and the Social Engineer Toolkit (SET) [37], provide essential capabilities enabling attackers to simulate official websites and collect user data. On the other hand, more recent toolkits like Evilginx, Modlishka, and Muraena, furnish attackers with advanced functionalities for conducting Man-in-the-Middle (MiTM) attacks. These contemporary toolkits successfully circumvent the limitations of multi-factor authentication, widely employed as a strategy in today's websites to counter phishing attacks [38].

In the meantime, the application of phishing toolkits can also be used to identify the phishing websites by researchers. Britt et al. [39] identified many phishing attacks based on the assumption that most phishing websites are built on various phishing kits instead of creating new phishing websites every time. Cui et al. [40] also argued that most phishing websites were the replicas or variations of previous ones. Orunsolu and Sodiya [41] detected phishing pages by using the approach that collects the features from phishing toolkits with a Signature Detection Module (SDM). Kondracki et al. [38] created a machine learning classifier to discover the presence of MiTM phishing toolkits, while Castano et al. [42] proposed a dataset containing the phishing toolkits and phishing websites created with these toolkits for phishing website identification.

B. BLACKLISTS

Blacklists are one of the most primary effective methods to protect against phishing attacks [9]. These lists serve as identifiers for malicious websites, functioning similarly to access control mechanisms. The feeds populating these lists can originate from user notifications, spam detection systems, and third-party sources [43]. A blacklist's effectiveness depends on several characteristics, the most important of which are its scope, size, speed, frequency of updating, and accuracy [38], [44]. Any known phishing URLs are entered in these lists and are used as control lists by browsers to prevent users from accessing them. The most popular blacklists in the past ten years of literature include Google Safe Browsing [7], [45], PhishTank [46], [47], and OpenPhish [48], [49]. These blacklists are most famous because most popular web browsers like Opera, Firefox, Safari, and Chrome, email service providers, and famous antivirus software like McAfee use these lists to filter out phishing or malicious websites. For the blacklist to be effective and efficient in indicating a phishing website, it must be updated regularly and quickly enough to protect the users from any possible phishing ahead.

However, this schema falls short in safeguarding users from phishing websites, owing to the minimal cost involved in generating a new URL [50] and its inability to detect zero-day phishing websites [51]. Sameen et al. proposed a method capable of detecting zero-day attacks by utilizing the lexical features of URLs, with the aim of enhancing the efficacy of existing blacklist-based mechanisms [15]. Nonetheless, phishers can exploit the vulnerabilities, commonly referred to as cloaking techniques, in anti-phishing blacklists to circumvent inclusion on these lists.

C. ANTI-PHISHING ECOSYSTEM

Many studies in the past have explored and discussed the various parts and components of the phishing or anti-phishing ecosystem [24], [52], [53], [54]. However, Oest et al. [32] are the first study to have explored and presented an overview of the anti-phishing networks as a whole, consolidated ecosystem. It was defined as being composed of several components that included the phisher, the underground phishing/cybercriminal economy, the organization that is being impersonated, the platform being used for messaging, the hosting platform, website owners, domain registrars, the organizations that are targeted indirectly, the phishing content, the victim, and the anti-abuse or anti-phishing entities (which include enterprise protection, blacklists, consumer protection, and the Anti-Phishing Community). Currently, data sharing between organizations is relatively uncommon [55], and existing studies provide no evidence of a protocol in place to facilitate such sharing. Consider a typical phishing campaign scenario: an attacker constructs a phishing website with a registered domain, hosts it on a cloud server, and then disseminates the phishing link via a social platform. Each entity in this scenario may individually detect and act upon the phishing URL, but without collaboration, their efforts remain disjointed. This lack of coordination inadvertently facilitates the attacker's mission, allowing them to sustain the attack with minimal effort. More importantly, each entity has unique information that can help detect the phishing website when these data can be safely and timely exchanged, which can achieve more proactive defense against phishing websites. Therefore, many researchers advocate for the deployment of ecosystem defenses to counteract the escalating trends in phishing attacks [55], [56], [57].

D. CLOAKING

Cloaking techniques are the techniques used to hide the real phishing content from web crawlers or bots that act as infrastructure for blacklists. However, the content remains visible to the human victims [27], [40]. When a phishing website suspects that a particular request has not come from a human but instead from a web crawler or bot, the website presents the crawler or bot with some benign webpage. Cloaking mechanisms are presented in some standard phishing kits available for criminals, with filters being applied on both the client side and the server side, which are based upon the HTTP request attributes and characteristics of the particular client devices or verifications [22], [23], [32] as well as some advanced fingerprinting from browser [58]. This is why some researchers have concluded that some devices and software are more capable of capturing flagged phishing material than others [44], [59]. With the nature of cloaking techniques, aforementioned strategies fail to detect the phishing websites with cloaking techniques. In the meantime, very limited researches shed the light on the detection methods on cloaking techniques. Invernizzi et al. [27] devised a methodology that involved accessing potential phishing websites exhibiting cloaking techniques, using multiple crawlers that emulate sophisticated legitimate user behavior. This approach was designed to detect server-side cloaking techniques employed by phishing websites. Extending this research, Zhang et al. [60] proposed a framework that leverages state-of-the-art static and dynamic code analysis to detect phishing websites utilizing client-side cloaking techniques. Despite enhancements in phishing website detection through these studies, the inherent latency in these mechanisms presents significant challenges when employed as protective strategies. Zhang et al. [61] advocate a proactive approach, proposing the intentional triggering of cloaking with specific payloads. This strategy, implemented as a browser extension, is designed to shield users from more sophisticated server-side cloaking. Nevertheless, its effectiveness remains confined to known cloaking techniques.

III. METHODOLOGY

A. NATURE AND TYPE OF RESEARCH

The current study's systematic literature review (SLR) methodology is designed using the PRISMA methodology (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). The PRISMA technique allows transparent review techniques and methodological reporting strategies. The reason for using this technique is that the objectives require the exploration of previous literature in an organized and methodological manner. The review process will allow the researcher to collect literary evidence on cloaking/evasion strategies and detection mechanisms for phishing so that the posed research objectives can be fulfilled [62].

B. SEARCH SOURCES AND KEYWORDS

For the search methodology, multiple databases have been used in this research. The databases selected in the current study are Web of Science (WoS), SCOPUS, and Google Scholar. In a systematic review, the keywords used for searching are another important factor to finalize in the initial stages. In order to ensure an extensive search, a relevant set of keywords must be used. A mix of 8 different keyword strings has been used to conduct the search process in the current study. The keyword strings used included ''cloaking techniques used in phishing websites,'' ''evasion techniques used in phishing websites,'' ''server-side cloaking techniques for phishing,'' ''server-side evasion techniques for phishing,''

"client-side cloaking techniques for phishing," "client-side evasion techniques for phishing," "Anti-phishing ecosystem," and "Phishing blacklists."

C. INCLUSION EXCLUSION CRITERIA

The inclusion criteria can be summarized as follows:

1) Papers published between 2012 and 2022.
2) Another inclusion criterion is that only peer-reviewed papers will be included.
3) Journal papers and conference papers will be included.
4) Papers published in the English language will be included in this paper.

The exclusion criteria for the shortlisted studies are as follows:

1) Any papers published before 2012 or after 2022 are excluded.
2) Papers published in languages other than English are excluded.
3) Any books, websites, reports, company profiles, working papers, etc., will not be included in the review.
4) Non-peer-reviewed literature will be excluded.

D. DATA ABSTRACTION

Excel spreadsheets are used for the abstraction of data. For the papers in the final review, data is extracted into a spreadsheet by full-text analysis. Some features extracted include title, authors, year, abstract, methodology, main objective, main strategy used, main findings, theoretical implications, and practical contribution.

IV. RESULTS

A. SEARCH RESULTS

For analysis, a total of 122 papers were collected using the retrieval process on the selected databases. 72 of these papers were extracted from SCOPUS and 50 from WoS. Furthermore, analysis of the reference list of the selected 122 papers led to the extraction of 26 other papers, making a total of 148 papers. As shown in Fig. 2, the first filtration was applied to remove duplicates or grey literature from the data set, reducing the number of papers to 92. Next, the titles and abstracts of the 92 papers were analyzed, and 45 were selected to go on to the full-text analysis stage. When trying to access the full text of the selected 45 papers, 12 papers were dropped due to the non-availability of the full text. Full-text analysis of 33 papers was carried out, and 30 were included in the final data set as listed in Table 1. The reason for dropping out of the three papers was that they were review papers.

B. CHARACTERISTICS OF THE INCLUDED PAPERS

1) YEARLY DISTRIBUTION

The range of time for this survey was from 2012 to 2022. Fig. 3 below shows each year's contribution in terms of the number of papers. No papers from 2013 or 2015 made it to the final list of papers included in the review. One paper from 2022 was included. Two papers each from 2012, 2016, and 2018 were included. Three papers, each from 2017 and 2019,

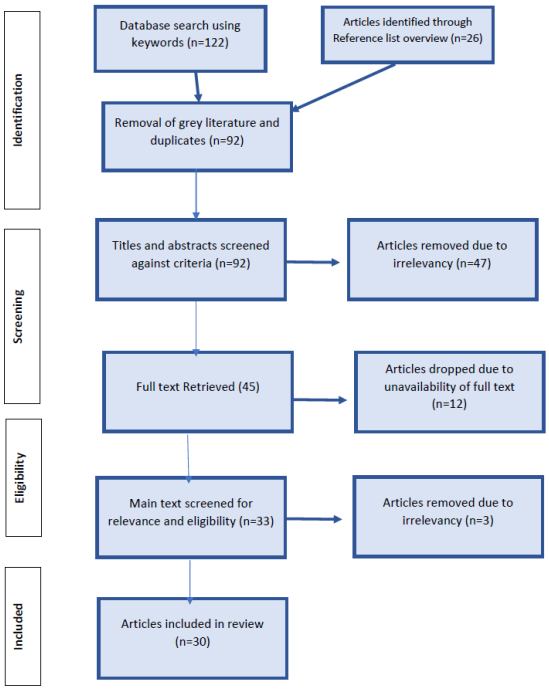

FIGURE 2. PRISMA flowchart.

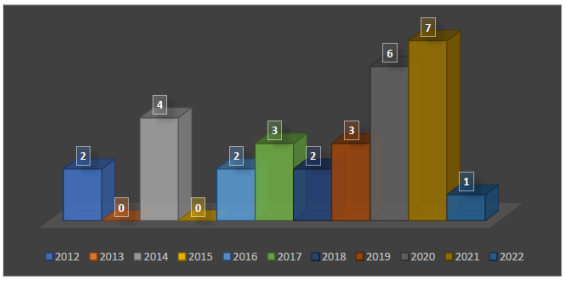

FIGURE 3. Yearly distribution.

were included. Four papers from 2014, six from 2020, and seven from 2021 were included. Hence, a major number of papers (14 out of 30) were from the past three years.

2) PAPER TYPES AND SOURCES

In this review, the conference papers and journal papers are included in the research. The reason for including conference papers is that the topic of the current review falls in the field of information technology, and most of the research in this domain is based on experimentation and projects that are presented more readily in the form of conference proceedings instead of journal articles. Fig. 4 below shows that out of the 30 included papers, 24 (80%) were conference proceedings, and only 6 (20%) were journal papers. Consequently, the inclusion of the conference proceedings is justified. If similar past studies are consulted, they also tend to include conference papers in their review process [21], [63], [64].

TABLE 1. List of included papers.

Authors	Year	Title	Source
Aggarwal et al.	2012	PhishAri: Automatic real-time phishing detection on Twitter	IEEE
Marchal et al.	2012	Proactive discovery of phishing-related domain names	Springer
Abdelhamid et al.	2014	Phishing detection based associative classification data mining	ScienceDirect
Lee et Al.	2014	Poster: Proactive blacklist update for anti-phishing	ACM
Marchal et al.	2014	PhishStorm: Detecting phishing with streaming analytics	IEEE
Tsalis et al.	2014	Browser blacklists: the Utopia of phishing protection	Springer
Han et al.	2016	Phisheye: Live monitoring of sandboxed phishing kits	ACM
Invernizzi et al.	2016	Cloak of visibility: Detecting when machines browse a different web	IEEE
Cui et al.	2017	Tracking phishing attacks over time	ACM
Duan et al.	2017	Cloaker catcher: a client-based cloaking detection system	Springer
Marchal et al.	2017	Off-the-hook: An efficient and usable client-side phishing prevention application	IEEE
Oest et al.	2018	Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis	IEEE
Shirazi et al.	2018	Kn0w Thy Doma1n Name" Unbiased Phishing Detection Using Domain Name Based Features"	ACM
Oest et al.	2019	Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists	IEEE
Peng et al.	2019	Opening the blackbox of Virustotal: Analyzing online phishing scan engines	ACM
Zhao et al.	2019	A decade of mal-activity reporting: A retrospective analysis of Internet malicious activity blacklists	ACM
Abdelnabi et al.	2020	VisualPhishNet: Zero-day phishing website detection by visual similarity	ACM
Bell and Komisarczuk	2020	An analysis of phishing blacklists: Google safe browsing, OpenPhish, and PhishTank	ACM
Maroofi et al.	2020	Are You Human? Resilience of Phishing Detection to Evasion Techniques Based on Human Verification	ACM
Oest et al.	2020	PhishTime: Continuous Longitudinal Measurement of the Effectiveness of Anti-phishing Blacklists	ACM
Oest et al.	2020	Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale	ACM
Rao et al.	2020	CatchPhish: detection of phishing websites by inspecting URLs	Springer
Acharya and Vadrevu	2021	PhishPrint: Evading Phishing Detection Crawlers by Prior Profiling	ACM
Bijmans et al.	2021	Catching phishers by their bait: Investigating the dutch phishing landscape through phishing kit detection	ACM
Kim et al.	2021	Security Analysis on Practices of Certificate Authorities in the HTTPS Phishing Ecosystem	ACM
Kondracki et al.	2021	Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits	ACM
Lin et al.	2021	Phishpedia: a hybrid deep learning-based approach to visually identify phishing webpages	ACM
Samarasinghe and Mannan	2021	On cloaking behaviours of malicious websites	ScienceDirect
Zhang et al.	2021	Crawlphish: Large-scale analysis of client-side cloaking techniques in phishing	IEEE
Acharya and Vadrevu	2022	A Human in Every APE: Delineating and Evaluating the Human Analysis Systems of Anti-Phishing Entities	Springer

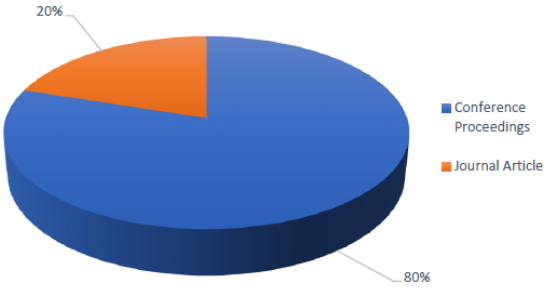

FIGURE 4. Type of papers.

Two journal articles are taken from IEEE journals, Transactions on Computers and Transactions on Network and Service Management. Two journal articles are sourced from Springer and were published in the Journal of Ambient Intelligence and Humanized Computing. The last two journal articles were sourced from ScienceDirect and published in Expert Systems with Applications and Computers & Security journals. The various conferences and their sources are also presented in Table 2.

In summary, 16 out of 30 included articles were from ACM, followed by seven from IEEE, five from Springer, and two from ScienceDirect.

3) CO-AUTHORSHIP OCCURRENCE AND NUMBER OF AUTHORS

A total of 110 authors were found to be part of the 30 included papers. Fig. 5 shows a network analysis of the ten most commonly appearing authors and formulates a network analysis of co-authorship between them. Gail-Joon Ahn and Adam

TABLE 2. Type, source, and number of paper from each source.

Journal Articles	IEEE	Transactions on Network and Service Management	(Marchal et al., 2012)
		Transactions on Computers	(Marchal et al., 2014)
	Springer	Journal of Ambient Intelligence and Humanized Computing	(Duan et al., 2017; Rao, Vaishnavi, & Pais, 2020)
	ScienceDirect	Expert Systems with Applications	(Abdelnabi, Krombholz, & Fritz, 2020)
		Computers & Security	(Samarasinghe & Mannan, 2021)
Conference Proceedings	IEEE	2012 eCrime Researchers Summit	(Aggarwal et al., 2012)
		IEEE Symposium on Security and Privacy (2016, 2019, 2021)	(Oest et al., 2018; Zhang, et al., 2020; Invernizzi et al., 2016)
		APWG Symposium on Electronic Crime Research	(Oest et al., 2019)
	ACM	USENIX Security Symposium (29th and 30th) 5	(Oest, Safaei, et al., 2020; Oest, Zhang, et al., 2020; Acharya & Vadrevu, 2021; Bijmans et al., 2021; Lin et al., 2021)
		ACM Asia Conference on Computer and Communications Security (2019, 2021)	(Zhao et al., 2019; Kim et al., 2020)
		ACM SIGSAC Conference on Computer and Communications Security (2014, 2016, 2020, 2021)	(Lee, Lee, Chen, & Tseng, 2014; Han et al., 2016; Abdelnabi, Krombholz, & Fritz, 2020; Kondracki et al., 2021)
		Proceedings of the 23rd symposium on access control models and technologies	(Shirazi, Bezawada, & Ray, 2018)
		Proceedings of the 26th International Conference on World Wide Web	(Cui et al., 2017)
		Proceedings of the ACM Internet Measurement Conference	(Peng, Yang, Song, & Wang, 2019)
		Proceedings of the Australasian Computer Science Week Multiconference	(Bell & Komisarczuk, 2020)
		Proceedings of the Internet Measurement Conference	(Maroofi et al., 2020)
	Springer	International Workshop on Recent Advances in Intrusion Detection	(Marchal et al., 2014)
		International Conference on E-Business and Telecommunications	(Tsalis et al., 2014)
		International Conference on Detection of Intrusions and Malware and Vulnerability Assessment	(Acharya & Vadrevu, 2022)
			30

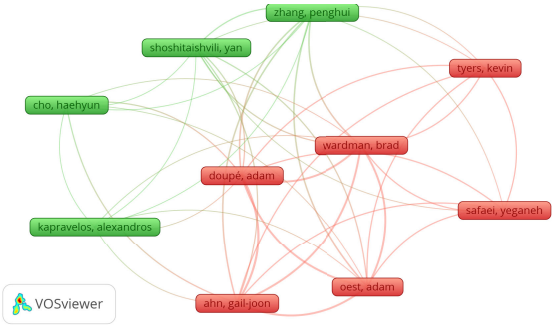

FIGURE 5. Co-authorship analysis.

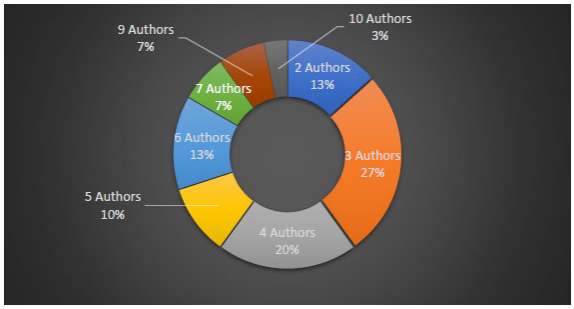

FIGURE 6. Number of authors per paper.

Doupé were the authors that appeared in most papers, followed by Adam Oest and Brad Wardman.

As for the number of authors per paper, most papers included more than three authors (60%). It can be seen in Fig. 6 that 13% of papers had two authors, 27% had three authors, and the rest, 60%, had more than three authors. To elaborate, 20% of papers involved four authors, 10% involved five authors, 13% involved six authors, 7% had seven authors, 7% had nine authors, and 3% had ten authors.

C. THEMATIC FINDINGS

Fig. 7 presents a depth analysis of the titles and abstracts of the papers that have been included in this review. The figure shows the ten most repeated words or phrases in the included papers' titles and abstracts, which have come out to be phisher, phishing blacklist, phishing detection system, blacklist update, phishing web page, cloaking, and other search words that have been used, indicating that the papers are most relevant.

The papers included in this review have been divided into two major themes according to the objectives of the current study: cloaking/evasion techniques and phishing website ecosystems. Thematic distribution of reviewed papers is shown in Table 3. The cloaking/evasion techniques that have been reported include client-side cloaking techniques, server-side cloaking techniques, manipulation of URLs, content-based cloaking techniques, and detection of client-side and server-side cloaking. The phishing website ecosystem that

TABLE 3. Thematic distribution of reviewed papers.

Themes	Sub-Theme	%	Refs
Phishing Website Ecosystem	Anti-Phishing Ecosystem	13%	[32], [55], [56], [65]
	Phishing Blacklists	30%	[3], [23], [40], [66]–[71]
	Phishing Toolkits	13%	[3], [32], [38], [44]
Cloaking/Evasion Techniques	Server-Side Cloaking Techniques	17%	[23], [26], [27], [32], [56]
	Client-Side Cloaking Techniques	13%	[22], [23], [56], [60]
	URL Manipulation for Cloaking	23%	[25], [54], [67], [69], [72]–[74]
	Content-based Cloaking Techniques	3%	[54]
	Client-Side and Server-Side Detection	47%	[25]–[27], [38], [40], [53], [54], [59], [67]–[69], [72], [73], [75]
	Other Evasion Techniques	13%	[58], [75]–[77]

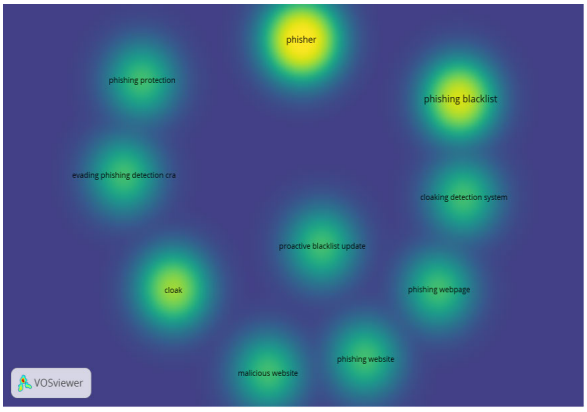

FIGURE 7. Word frequency analysis of included titles.

has been reported includes anti-phishing ecosystem concepts, phishing blacklists, and phishing toolkits.

V. PHISHING WEBSITE ECOSYSTEM AND EVASION/ CLOAKING TECHNIQUES

Several cloaking/evasion techniques and detection strategies are mentioned in this study's reviewed papers. In addition, the objectives, strength as well as the weakness of these reviewed papers are shown in Table 4. These findings are discussed and presented below.

A. ANTI-PHISHING ECOSYSTEM

Oest et al. [32] provided an overview of the anti-phishing ecosystem from the perspective of criminals, shedding light on its various components. The study revealed that the ecosystem extends beyond the victims, organizations being impersonated, and phishers themselves. Despite the involvement of multiple security communities and strategies, the authors emphasized that phishers possess awareness and knowledge of the countermeasures employed against them. Consequently, they are able to optimize the effectiveness of their cloaking strategies, resulting in a higher number of successful attacks. Thus, Oest et al. [32] argued that the research community must gain a comprehensive understanding of the strategies and pathways employed by phishers in order to identify weaknesses in the overall ecosystem. They further recommended the combination of malicious URL detection with techniques for identifying the source of attacks, thereby improving the ecosystem's protection and efficiency.

In another study, Oest et al. [55] highlighted how phishers exploit weaknesses and gaps in the ecosystem, leading to a significant daily volume of attacks. The researchers proposed a framework called Golden Hour, which enables the passive measurement of victim traffic to phishing websites and proactively prevents a substantial number of account compromises. Additionally, their findings indicated that a small number of sophisticated campaigns accounted for over 89% of the attacks. Therefore, future research should focus on developing strategies specifically targeted at these types of attacks. Kim et al. [65] discussed the critical and significant role of certification authorities in the anti-phishing ecosystem due to the rapid increase in HTTPS phishing attacks. Recognizing this trend, Oest et al. [56] concluded by calling for collaborative efforts to enhance data sharing and response times when dealing with reported phishing websites, as they observed emerging trends in the evolving ecosystem.

B. PHISHING BLACKLISTS

Marchal et al. [67] presented a mechanism for proactively discovering domain names related to phishing activities. This strategy was based on natural language-based modeling for building proactive blacklists. It was claimed that the proactive blacklist would be able to detect phishing websites efficiently compared with the reactive update method, but further testing is required. Another study also presented a framework called PhishTrack that proactively found phishing URLs based on redirection tracking and form tracking [68]. Marchal et al. [69] also discussed using another framework that proactively created a blacklist for malicious websites based on the knowledge that phishers only violate a specific part of the URL. Tsalis et al. [70] conducted their study when the trend of online shopping and mobile devices for

TABLE 4. Comparison on the strength and weakness of reviewed papers.

Authors	Year	Objective	Main Methods Used	Strength	Weakness/Limitation
Oest et al.	2018	To understand the tactics and motives of sophisticated cybercriminals for enhancing anti-phishing systems by analyzing real-world data and server-side evasion techniques via .htaccess files.	Data Anaylsis and empirical Experiment	Identified five fliters used as server-side cloaking techniques including Deny IP, Allow IP, Hostname, Referrer and User Agent.	A skewed APWG database, unavailability of .htaccess files, and potential bias in reported malicious URLs.
Oest et al.	2020	To measure the life cycle of large-scale phishing attacks and analyze their progression using expansive datasets.	Data Anaylsis and empirical Experiment	Provided extensive visibility into phishing hostnames, reveals significant attack duration, highlights the prominence of large attacks, showcases the longevity of phishing campaigns, and develops proactive mitigation strategies.	Single-company collaboration, privacy restrictions limiting shared findings, overlooked phishing web content, targeting specificity, challenges scaling redirection link correlations, and potential visibility issues due to reliance on anti-phishing vendors' URL data.
Kim et al.	2021	To understand the security practices of CAs in the HTTPS ecosystem including Issuance, Revocation and Re-issuance issues.	Data Anaylsis and empirical Experiment	Provided a comprehensive examination of CA security practices, revealing significant security concerns and the effectiveness of HTTPS phishing attacks.	Limited to DV certificates but there are evidences of using OV and EV in phishing websites.
Oest et al.	2020	To assess the ecosystem's vulnerability to modern phishing attacks, focusing on blacklisting coverage, speed, and consistency.	Data Anaylsis and empirical Experiment	Proposed a systematic, flexible, and automated method for long-term evaluation of anti-phishing defenses, identifying gaps and testing emerging threats for continuous user protection.	The study has potential bias in phishing site appearance, lacks positive domain reputation consideration, and covers a limited scope of phishing configurations.
Zhao et al.	2019	To provide a systematic characterization and temporal analysis of reported internet malicious activities using public blacklists, while leveraging machine learning for classification.	Machine Learning Techniques	Uniquely combined machine learning with historical data to create a decade-long malicious activity dataset, freely available for public research, offering profound insights into persistent online threats.	The omission of popular blacklists, potential bias towards specific threats, sparsity in time coverage, and inaccuracies in IP-Country mappings due to the sporadic nature of archival records.
Han et al.	2016	To present a novel approach for sandboxing live phishing kits to comprehensively assess real-world phishing attacks, criminals, victims, and security responses.	Built a honeypot system.	Pioneered a honeypot system to analyze and disarm phishing kits, measures their effective lifetime, and distinguishes victims, attackers, and third-party visitors.	The challenge of precisely separating phishing applications from other malicious files and the potential erroneous removal of small phishing kits during the process.
Oest et al.	2020	To examine the vulnerability of ecosystems to phishing, including blacklisting coverage, speed, consistency, and security implications.	Data Anaylsis and empirical Experiment	Effectively demonstrated the speed and coverage of blacklists, highlighted Google's rapid response, and exposed evasion techniques' impact on detection.	Unaltered phishing website appearances, lacking positive domain reputations, and limited experimentation on available phishing configurations.
Cui et al.	2017	To analyze the replication patterns in phishing attacks, assess the effectiveness of current prevention techniques, and propose enhancements.	Clustering Algorithm on Structure of DOMs	Presented an effective method to detect replicated phishing attacks, achieving 90% detection rate with low false positives, potentially enhancing phishing defense strategies.	Despite the effectiveness of the proposed method in catching replicas of known phishing sites, its future performance could be hampered by thorough modifications from attackers, necessitating further adaptive strategies.
Marchal et al.	2012	To introduce a proactive approach for detecting potential phishing-related domain registrations using natural language modelling techniques.	Natural Language Modelling Techniques	A proactive domain-generation tool to detect future phishing sites, leveraging a Markov chain model, linguistic features, and semantic tools, significantly augmenting existing anti-phishing measures.	Implementing and improving the domain checker.
Lee et al.	2014	To improve real-time detection of phishing threats by proposing a proactive framework, PhishTrack, to update phishing blacklists.	URL Redirection & Form Tracking	Viability of real-time phishing URL discovery using existing blacklists, introduces a proactive update mechanism, and demonstrates promising results with PhishTrack.	Keeping up with rapidly changing phishing threats and enhancing blacklisting remains challenging.
Marchal et al.	2014	To introduce PhishStorm, an automated real-time phishing detection system that uses intra-URL relatedness and machine learning for efficient phishing URL detection.	URL lexical analysis	Presented PhishStorm, an efficient URL detection system achieving 94.91% classification accuracy and a 1.44% false positive rate. It leverages Big Data streaming architectures for real-time analytics.	An inability to detect certain obfuscated URLs and data constraints from Google Trends and Yahoo Clues, impacting accuracy and processing speed.
Tsalis et al	2014	To evaluate and compare phishing protection mechanisms in popular Android and iOS web browsers with their desktop counterparts.	Data Anaylsis and empirical Experiment	Extensively assessesdanti-phishing measures across multiple platforms, revealing weaknesses, highlighting disparities in browser protection, and informing future security enhancements.	The measurement is limited coverage in anti-phishing blacklists.
Bell and Komisarczuk	2020	To measures and compares the effectiveness, size, update speed, and overlap of three key phishing blacklists: Google Safe Browsing, OpenPhish, and PhishTank.	Data Anaylsis and empirical Experiment	A detailed comparison of three key phishing blacklists: GSB, OP, and PT, offering insights on their uptake, dropout, and overlap, with GSB showing impressive volume and OP demonstrating swift detection rates.	Encountering limitations due to GSB's URL encryption, lack of false positives analysis, and unexplored impacts of blacklisting.
Bijmans et al.	2021	To figure out how do phishing tool kits impact the phishing landscape and how often they are used.	Data Anaylsis and empirical Experiment	Offered an empirical investigation of the Dutch phishing landscape, identifying prevalent tactics, swift detection methodologies, and effective countermeasures for future interventions.	Focusing solely on HTTPS phishing domains, recognizing only certain phishing domain types, and potential inaccuracies in phishing kit detection.
Kondracki et al.	2021	To demonstrate first analysis of MITM phishing toolkits used in the wild and use intrinsic network-level properties to identify the phishing websites.	Machine Learning Techniques	Successfully developed a high-accuracy classifier to detect MITM phishing toolkits and revealed significant blocklist deficiencies.	Focusing on the network features to build a classfier rather than the features on the application layer.
Samarasinghe and Mannan	2021	To understand cloaking behaviors across a broad set of websites, and develop effective, scalable detection techniques for cloaked malicious sites.	Evaluation dissimilarities of website features	Innovatively improved detection of cloaked malicious sites with a broader set of domains, providing an 80% detection rate and effectively utilizing domain generation engines.	The crawler itself may be filtered by cloaking techniques because of the use of headless browser and/or search engine crawler. It is also limited to a certain cloaking technique.
Invernizzi et al	2016	To investigate blackhat cloaking techniques that compromise web services, develops an anti-cloaking system with high accuracy, and characterizes threats in the wild.	Machine Learning Techniques	Provided a comprehensive examination of blackhat cloaking techniques, develops a high-accuracy de-cloaking crawler and classifier, and identifies key evasion methods.	Primarily on current blackhat practices, potentially overlooking emerging fingerprinting techniques not yet deployed.
Oest et al.	2019	To measure how cloaking techniques impacts the effectiveness of blacklists across major desktop and mobile browsers by reporting the websites with cloaks to 10 different anti-phishing entities.	Data Anaylsis and empirical Experiment	Revealed the effectiveness of several both cloakings against blacklists, agility of Google Safe Browsing, and lack of data sharing between key players.	Limited by its focus on default browser protections, exclusion of certain detection methods, and unexplored submission channels.
Maroofi et al.	2020	To study the resilience of anti-phishing entities to three advanced anti-analysis techniques based on human verification: Google reCAPTCHA, alert box, and session-based evasion.	Data Anaylsis and empirical Experiment	Uncovered major server-side anti-phishing bots' limitations, demonstrates Google Safe Browsing's efficacy, and exposes Google re-CAPTCHA's misuse in shielding phishing content.	Potential underrepresentation of evasion techniques in public blacklists, challenges in measuring these techniques' popularity.
Abdelnabi et al.	2020	To introduce VisualPhishNet, a novel phishing detection framework using a triplet CNN, that enhances visual similarity-based detection of unseen phishing pages.	Deep Learning Techniques	Enhanced image-based visual similarity detection for zero-day phishing, introducing VisualPhish, the largest dataset, and VisualPhishNet, a deep learning model, significantly outperforming previous methods.	Struggling with incorrect website matches and false positives, especially for phishing pages with dissimilar appearances, outdated designs, or pop-up windows.
Marchal et al.	2017	To develop and evaluate 'Off-the-Hook', a new real-time browser-based phishing detection approach, addressing existing solution limitations.	Machine Learning Techniques	A client-side phishing detection tool, a novel set of features for detection, a fast target identification technique, comprehensive evaluation, and positive usability studies.	Limitations include issues with term extraction, incorrect domain splitting, inconsistent abbreviations, and misclassification of legitimate and unrelated-content hosting sites.
Aggarwal et al.	2017	To detect phishing on Twitter in real-time using a system called PhishAri, which combines Twitter-specific and URL-based features, providing a Chrome browser extension for users.	Machine Learning Techniques	PhishAri, the developed system, outperforms standard blacklisting mechanisms and Twitter's defense system, detecting 80.6% more URLs with a 92.52% accuracy. It also offers a RESTful API and a Chrome extension.	PhishAri currently only analyzes tweets from public users and lacks a backend database for faster lookup. Future improvements include OAuth integration with Twitter and database enhancement.
Shirazi et al.	2018	To detect phishing websites using a machine learning approach, focusing on domain name relationships to key phishing website elements, eliminating dataset biases.	Machine Learning Techniques	Used seven domain name-based features achieving 97% classification accuracy, and detection rates of 97-99.7% for live black-listed URLs, demonstrating robustness and real-time suitability.	The robustness of the machine learning algorithms against newer phishing attacks is yet to be explored.
Rao et al.	2020	To propose CatchPhish, a lightweight application that predicts URL legitimacy using URL, hostname, and TF-IDF features without visiting websites.	Machine Learning Techniques	CatchPhish, independent of third-party services and source code, delivers high accuracy (94.26%-98.25%) and low response times using hybrid features and Random Forest classification.	The model could misclassify phishing sites on free or compromised servers, ignore visual mimicry in source code or images, and miss shortened URLs.
Peng et al.	2019	To understand the reliability and labeling process of VirusTotal's online scan engine and its third-party vendors on phishing URLs.	Data Anaylsis and empirical Experiment	By setting up and submitting phishing URLs for scanning, this study provides new insights into VirusTotal's functionality and labeling quality.	"The experiment's use of long and ""fresh"" domain names might affect detection accuracy, and scanners might perform better on sites that already had victims."
Duan et al.	2017	To mitigate IP and SEM cloaking, offering client-based real-time cloaking detection services using the Simhash-based Website Model.	Simhash-based Website Model	Proposed a system that accurately detects IP and SEM cloaking in real-time, offering efficient and privacy-preserving services, and preventing click fraud.	The study leaves the representation of URL features for future work and automating incentive analysis. It also recognizes SWM availability as a challenge.
Zhang et al.	2021	To develop a framework to detect and categorize the cloaking types and measures the impact of the cloaked phishing websites.	Data Anaylsis and empirical Experiment	Provided an in-depth analysis of client-side JavaScript used by phishing websites, identifying and categorizing evasion techniques, and measuring their prevalence.	CrawlPhish needs a feed of phishing URLs and might miss sophisticated server-side cloaking techniques. Its cloaking categorization can misclassify evasion codes, and certain execution limitations exist.
Acharya and Vadrevu	2022	To evaluates APEs, revealing strong evidence of human analysis systems and identifying weaknesses that allow evasive attacks.	Data Anaylsis and empirical Experiment	Identified the presence of human analysis systems in major APEs and exposed exploitable weaknesses, offering mitigation suggestions for improved security.	The estimates of human involvement in APEs may be conservative due to relying on CAPTCHA-solving activity; actual human-analysis rate could be higher.
Acharya and Vadrevu	2021	To build a framework named PhishPrint to enable the evaluation of such web security crawlers against multiple cloaking attacks.	Data Anaylsis and empirical Experiment	Constructed a scalable framework for evaluating web security crawlers, discovered weaknesses, and performed thorough disclosure procedures.	The study doesn't cover certain phishing scenarios, may overestimate a crawler's infrastructure, and could potentially aid adversaries.
Lin et al.	2021	To accurately identify phishing websites with visual explanation.	Deep Learning Techniques	Proposed Phishpedia, a deep learning approach for phishing detection, offering perfect logo identification, low runtime overhead, unbiased dataset, and annotated visualizations.	Reimplemented baseline approaches may affect performance; cloaking of phishing websites could disrupt VirusTotal engines.

social media was still catching up. The work revealed that the users of Android and iOS were not efficiently protected against phishing attacks. The work was primarily based on evaluating the web browsers used on the Android, Windows, and iOS platforms and revealed that only a few browsers on iOS and Android were adequately protected against possible phishing attacks. It was also found that even if the browsers on mobile devices were providing the protection, it was not as effective as in the desktop versions. Past research, including work by Cui et al. [40] and Han et al. [3], indicates that attackers can circumvent blacklist-based protections by subtly modifying the DOM of web pages and re-launching attacks on new domains and servers. In addition, Bell and Komisarczuk [71] were the first to explore Google Safe Browsing, OpenPhish, and PhishTank regarding the dropout ratio, uptake procedures, lifetimes, and overlaps of URLs present in them to understand the top 3 blacklists. The study by Zhao et al. [66] revealed that online prevention systems based solely on blacklists might fail as they are powerless when faced with persistent threats that may originate from a small number of sources. Moreover, they also indicate that the speed at which these lists are updated is not efficient enough to protect the users.

Abdelhamid et al. [53] highlighted the weakness of blacklists in terms of efficiency. The researcher discusses that the strategy that all blacklists work on is comparing the URL with already indexed and known malicious websites. However, as per Abdelhamid et al. [53], blacklists are slow to discover newly created URLs to capture phishing data. Therefore, phishers can successfully harm a wide number of users of the WWW before being detected by the blacklists. It was also suggested that heuristic-based detection of newly created malicious websites is more proactive than existing blacklists. Oest et al. [23] improved the performance of blacklists by proposing and implementing a framework that detects phishing websites that were repeatedly unidentified and reported for over 2800 new websites. It was concluded that long-term empirical measurements methodologically led to effective and more potent detection in the anti-phishing ecosystem. The study also highlighted weaknesses of the blacklists in terms of the detection of a class of evasion techniques that used behavior-based JavaScript. Bell and Komisarczuk [71] also conducted a similar study to Zhao et al. [66]. They analyzed the top 3 phishing blacklists over 75 days of experimentation to analyze the URLs' characteristics like dropout, uptake, lifetimes, and overlap. It was found that all three blacklists may be prematurely dropping out URLs, leaving users unprotected, due to the fact that all three blacklists had a significant number of reappearance of URLs within 24 hours of dropping off. The analysis also concluded that while OpenPhish was small, it had a 90% chance of flagging a phishing website before PhishTank.

C. PHISHING TOOLKITS AND COUNTERMEASURES

Several papers reviewed in this study discuss phishing toolkits and the countermeasures or techniques used to identify and protect users from phishers using these toolkits. Some commonly known countermeasures for phishing toolkits include redirection or shortening URLs, randomizing URLs using human verification systems, and code obfuscation [32]. Han et al. [3] designed and discussed implementing a honeypot system explicitly designed to disarm phishing toolkits in their study. The researchers conducted experiments that took around five months to understand and measure the lifecycles of attacks using these tools. It was one of the first successful attempts to measure a phishing toolkit's lifetime. Moreover, this study contributed to literature and practice as it was one of the first to effectively identify the attacker, the victim, and the third-party visitors, from the traffic.

Bijmans et al. [44] discuss that the availability of easy-to-use and deployed phishing kits has increased the incidence of phishing as criminals find it easy to harvest user information by using these tools and creating fraudulent websites. Bijmans et al. [44] investigated the Dutch phishing landscape and used an empirical research strategy to study the various phishing campaigns using the fingerprints of phishing kits. The study leveraged the information that the phishers used TLS certificates and found 1363 confirmed domains that used such kids within four months. The researchers found that most domains remained online for about 24 hours. However, most of them stayed online for much longer. The researchers also examined the effectiveness and validity of their framework using APWG data, revealing that the framework could detect phishing websites of various types swiftly. Moreover, it is also revealed that there are a countable number of types of different kits that are in use in the Dutch phishing landscape, as the study presented a deep insight into the techniques, tactics, and procedures being used by phishers to provide policymakers with an opportunity to improve anti-phishing initiatives. Kondracki et al. [38] evaluated using MiTM phishing toolkits, one of the latest evolutions in this domain. In these toolkits, the online services of the actual website are mirrored, and the live content is used to extract secret information and credentials from the users. These tools have made the lives of the phishers even more manageable, as they automate the procedure of harvesting the sessions and improve the believability of the malicious websites for the users. The study also highlighted some of the intrinsic network-level properties of MiTM toolkits and developed a machine-learning classifier that showed 99.9% accuracy in detecting such toolkits.

D. CLIENT-SIDE CLOAKING TECHNIQUES

Client-side cloaking primarily employs JavaScript-based front-end techniques to ascertain user legitimacy, thereby circumventing detection by anti-phishing entity crawlers. Maroofi et al. [22] detailed an evasion strategy that leverages alert boxes to collect data. This approach involves phishers creating JavaScript-based alert boxes, thereby restricting user interaction with the webpage until they meet certain stipulations. These prerequisites could range from sign-in credentials and email addresses to other sensitive

information exploitable for financial gain. For instance, as Maroofi et al. [22] discussed, a spurious PayPal website might utilize alert box evasion techniques, presenting alerts suggesting the user is already signed in, thereby prompting them to sign in again for sustained access. Additional client-side evasion techniques, as reported by researchers like Maroofi et al. [22] and Oest et al. [56], include session-based and captcha-based evasion strategies. Captcha-based evasion attempts to distinguish a human from a web crawler via captcha tests, such as Google reCAPTCHA. The detection of a crawler keeps the phishing content concealed. Simultaneously, the session-based strategy necessitates user engagement—whether clicking a button to initiate a chat or inputting credentials—to establish a session before revealing the phishing content. If such interaction is not forthcoming, users are redirected to a benign landing page to circumvent possible detections by APEs. In a notable development, Oest et al. [23] recognized a unique client-side evasion technique that verifies user authenticity through mouse movement detection. Zhang et al. [60] conducted a systematic investigation of these client-side cloaking techniques employed by modern phishing websites. Utilizing a framework called CrawlPhish, they identified three primary types of client-side cloaking techniques—user interaction, fingerprinting, and bot behavior—commonly deployed on a large scale. User interaction includes aspects such as pop-up windows, mouse detection, and click-throughs. Fingerprinting encompasses elements like Cookies, Referrers, and User-Agents. Bot behavior involves timing and randomization, where, for instance, the phishing content is not displayed until a randomized time or after certain times of visits to the webpage. This ensures only real users who are able wait or revisit a webpage can view the content, while APEs' crawlers are effectively filtered out.

E. SERVER-SIDE CLOAKING TECHNIQUES

Primarily, server-side cloaking exploits the characteristics of HTTP requests to discern whether the request originates from a potential victim or a detection system. A study conducted by Invernizzi et al. [27] delved into various types of cloaking mechanisms, including network, browser, and context strategies. Their findings highlighted a multitude of discrepancies in phishing content that often elude detection by web crawlers. This underscores the necessity of extending beyond merely investigating and comparing webpage semantics. The reason being, numerous phishers have devised cloaking tactics that extract crucial values from HTTP, such as the referrer, header, and user-agent, thereby displaying different content to human users and crawlers. Consequently, search engines frequently become victims of these cloaking techniques [56]. Samarasinghe and Mannan [26] elaborated that these cloaked websites are instrumental in delivering malicious content that victimizes users. Interestingly, they discovered that 22% of the cloaked domains managed to remain successful by distinguishing different user-agents in HTTP headers. Supporting this finding, Oest et al. [23], [32], [56] reported that server-side-based cloaked websites, which filter traffic using various HTTP request criteria, evade swift detection by blacklists and anti-phishing ecosystems. This evasion, in turn, enables them to successfully pilfer valuable client data.

F. URL MANIPULATION CLOAKING TECHNIQUES

Phishing websites frequently resort to URL manipulation, a method widely discussed in literature. In this scheme, phishers adopt URLs bearing a striking resemblance to the original brand websites [73], thereby evading web crawlers and duping users into divulging sensitive information [25], [67], [69]. Marchal et al. [25] dissect the exploitation of URL structure, highlighting that the primary component manipulated by phishers is the subdomain within the fully qualified domain name (FQDN). Remarkably, phishers wield absolute control over the subdomain, setting its value at will. They also tinker with other components such as the query and path, as detailed in the FreeURL report by Marchal et al. [25]. Although initially employed as a protective measure, URL obfuscation has been recognized for its susceptibility to manipulation, particularly through the shortening of phishing website URLs, thereby concealing malicious content in plain sight [54], [72]. Marchal et al. [25] investigated the various components tampered by phishers and discovered hundreds of phishing sites in the process. Rao et al. [73] further indicated that attackers could create numerous URL variants using obfuscation techniques, thus necessitating regular updates of blacklists and whitelists. Emphasizing the importance of comprehending how phishers elude URL detection, Peng et al. [74] examined the labels and tags utilized by a renowned URL-based detector, VirusTotal, revealing its rather limited effectiveness. Marchal et al. [69] further classified the cloaking techniques employed in URLs into distinct categories: URL obfuscation with another domain, URL obfuscation with keywords, typosquatting or long domains, URL obfuscation with IP address, and obfuscation with URL shortener.

G. CONTENT-BASED CLOAKING TECHNIQUES

With the escalating prevalence of attacks emanating from social media, researchers, including Aggarwal et al. [54], have scrutinized the cloaking techniques employed by phishers on such platforms. These malicious actors frequently fabricate fake social media accounts on networking sites with the intent of generating clicks on phishing content, thereby facilitating user data capture. In their study, Aggarwal et al. [54] analyzed phishing content on Twitter and identified several Twitter-specific features—such as tweet length, hashtags, previous tweet counts, and account age—that could serve as indicative characteristics of potential phishing tweets. Concurrently, they observed that phishers often usurp trending topics and commence posting unrelated content, appending their tweets with the trending hashtag. This strategy enhances their tweet visibility since trending topics, which are location-specific, are invariably displayed on a Twitter user's homepage. Consequently, content modification or maintaining a more credible profile can serve as a cloaking

technique, potentially circumventing detection systems predicated on message content and account information.

H. CLIENT-SIDE AND SERVER-SIDE DETECTION

Numerous studies have been proposed for detecting phishing websites, aiming to establish a more proactive strategy that augments current protective measures. Phishing website detection relies either on client-side [25], [54], [59] or server-side [26], [27], [38], [40], [53], [54], [67], [68], [69], [72], [73], [75] systems, contingent upon their deployment. However, a majority of the existing detection mechanisms are server-based, sharing similar shortcomings with blacklists, such as latency in detection and user protection.While client-side mechanisms primarily function as browser extensions, offering real-time user protection, these also surmount another disadvantage of server-side detection mechanisms. Although the detection algorithm in the server-side approach is invisible to phishers, appearing as a 'black box', there is no assurance that a server or a crawler will fetch identical content due to the evasion techniques employed by phishers. In instances where the phishing kit or phisher detects an anti-phishing bot, benign content is displayed. This weakness is effectively mitigated by client-side phishing detection techniques as they capture the same content as users.

Additionally, current detection mechanisms utilize various techniques, with machine learning techniques—using a single or combination of domain-based, content, and network features to build classifiers for identifying unknown phishing websites—being predominant [25], [27], [54], [72], [73]. Other techniques include deep learning [75], [76]. For instance, Lin et al. [75] designed a detection framework based on visual similarity strategies using a hybrid deep learning approach. This approach visually identifies phishing websites, providing higher accuracy and explainable results in phishing webpage detection. Unlike many previous studies focusing solely on the similarity between phishing and benign websites, this study presents a more effective method addressing the limitations posed by dynamic changes and content updates of phishing webpages. However, this approach falls short when applied to websites created with templates or benign websites featuring logos of famous brands, and when some cloaking techniques are used. Abdelnabi et al. [76] discussed the high occurrence of phishing attacks in today's Internet ecosystem and presented a similarity-based detection method for trusted websites. They introduced a framework named VisualPhishNet, a similarity-based detection framework for phishing content developed using a triple Convolutional Neural Network (CNN). This network detects the presence of phishing content, such as pop-ups, capture pages, or newly injected HTTP within past websites, by identifying differences in the visual appearance of the newly injected code and visual matter. In the domain of visual similarity phishing detection, this method outperformed state-of-the-art procedures, demonstrating robust detection of evasion attacks.

Natural language modeling techniques [67], and various other algorithms and methods [26], [40], [59], [69] are also utilized for phishing detection. Notably, some detection mechanisms extracting features from existing phishing toolkits or websites have proven effective in detecting phishing websites in the wild [40], [52]. However, few detection strategies consider the presence of cloaking techniques and strive to bypass them [26], [27], [59], highlighting a common flaw in current detection strategies.

I. OTHER EVASION TECHNIQUES

Acharya and Vadrevu [77] conducted an in-depth analysis of the different Anti-Phishing Entities (APEs) in order to evaluate the effectiveness of recognizing crawlers and human analysts in detecting phishing websites. This study revealed an optimistic outlook for cybersecurity as it can be concluded that the APEs are robust in their detection capabilities due to the involvement of human analysts. However, some weaknesses in these human systems include a lack of incorporation of geolocation, weaknesses in client-device diversity, and other discrepancies that may make users vulnerable to cloaked attacks.

Acharya and Vadrevu [58] then discussed a new strategy of cloaking mechanisms known as advanced fingerprinting-based cloaking. In this process, the phishers hides the malicious webpage from the user until and unless the user's fingerprint is not similar to the ones collected from anti-phishing entities using WebGL, Canvas and Fonts as well as some network features. The server-side then decides whether the user is a crawler or a human and acts based on this perception. The researchers developed a phishing system to test the various online services provided by anti-phishing entities for weaknesses against advanced fingerprinting-based cloaked attacks. They found that the whole crawler ecosystem is poorly equipped to fight this battle. It was concluded that the crawlers lacks diversity and effective measures in terms of protection against such advanced fingerprinting-based cloaked attacks by phishers.

VI. DISCUSSION AND CONCLUSION

This paper uses the PRISMA strategy to conduct an SLR of the cloaking techniques and detection mechanisms used in the phishing ecosystem. For this purpose, 30 papers have been carefully reviewed and extracted from SCOPUS, WoS, and Google Scholar published in 2012–2022. The results indicated that many cloaking/evasion techniques are currently used by phishers and revealed that many strong and intelligent detection mechanisms are being used to flag phishing websites. However, they still fail to counter the sophisticated cloaking/evasion techniques and phishing toolkits that further allow the phishers to succeed in their attempts at lower costs. It has been identified that a small number of sources are responsible for more than 80% successful attacks. Therefore, detection mechanisms must be more proactive and focused on such sources and cloaking techniques, which is also supported by similar findings in recent studies [48], [52], [63], [78], [79], [80], [81].

The present study contributes theoretically by delineating and defining diverse elements and theories within the phishing ecosystem, including a novel exploration of cloaking techniques in the phishing literature. Despite these advancements, some limitations are worth noting. The investigation was confined to experimental research papers; future work could broaden the scope by incorporating conceptual and theoretical literature. Although this study aimed to provide a general overview of the field, it did not exhaustively address any singular strategy for cloaking or detecting phishing content. Additional limitations pertain to the keywords employed in the study, the databases consulted, the inclusion and exclusion criteria, and the year range considered. Future research could expand the temporal scope of the included research, utilize a larger number of databases, and diversify the types of literature examined—like book chapters and thesis documents—which also offer valuable insights.

Furthermore, future research could benefit from a concentrated examination of individual cloaking mechanisms or detection strategies. In spite of numerous proposed and discussed detection mechanisms, internet users remain vulnerable to an increasing number of phishing websites. Consequently, researchers should shift their focus to exploring the potential and hitherto unidentified cloaking and evasion techniques employed by attackers in real-world scenarios, rather than solely focusing on the enhancement of existing detection schemas.

REFERENCES

[1] B. Janet and R. J. A. Kumar, "Malicious URL detection: A comparative study," in *Proc. Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Mar. 2021, pp. 1147–1151.

[2] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, and E. Bursztein, "Data breaches, phishing, or malware: Understanding the risks of stolen credentials," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1421–1434.

[3] X. Han, N. Kheir, and D. Balzarotti, "PhishEye: Live monitoring of sandboxed phishing kits," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1402–1413.

[4] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Apr. 2016, pp. 537–540.

[5] K. Rekouche, "Early phishing," 2011, *arXiv:1106.4692*.

[6] A. Al-Ani, A. K. Al-Ani, S. A. Laghari, S. Manickam, K. W. Lai, and K. Hasikin, "NDPsec: Neighbor discovery protocol security mechanism," *IEEE Access*, vol. 10, pp. 83650–83663, 2022.

[7] H. Cui, Y. Zhou, C. Wang, X. Wang, Y. Du, and Q. Wang, "PPSB: An open and flexible platform for privacy-preserving safe browsing," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 4, pp. 1762–1778, Jul. 2021.

[8] J. Britt, B. Wardman, A. Sprague, and G. Warner, "Clustering potential phishing websites using DeepMD5," in *Proc. 5th USENIX Workshop Large-Scale Exploits Emergent Threats (LEET)*, 2012, p. 10.

[9] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or not phishing? A survey on the detection of phishing websites," *IEEE Access*, vol. 11, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

[10] L. Allodi, T. Chotza, E. Panina, and N. Zannone, "The need for new antphishing measures against spear-phishing attacks," *IEEE Secur. Privacy*, vol. 18, no. 2, pp. 23–24, Mar./Apr. 2020.

[11] FireEye Inc. (2018). *APT37 (Reaper) The Overlooked North Korean Actor*. A FireEye Special Report Milpitas, Cal. [Online]. Available: https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf

[12] Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside. (2021). *The United States Department of Justice*. Accessed: Apr. 8, 2023. [Online]. Available: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[13] (2022). *Anti-Phishing Working Group APWG*. Phishing Activity Trends Report. [Online]. Available: https://apwg.org/trendsreports/

[14] The Latest Phishing Statistics: Aag it Support. (2022). *AAG IT Services*. Accessed: Apr. 8, 2023. [Online]. Available: https://aag-it.com/the-latest-phishing-statistics/

[15] M. Sameen, K. Han, and S. O. Hwang, "PhishHaven—An efficient real-time AI phishing URLs detection system," *IEEE Access*, vol. 8, pp. 83425–83443, 2020.

[16] M. Khonji, Y. Iraqi, and A. Jones, "Enhancing phishing E-Mail classifiers: A lexical URL analysis approach," *Int. J. Inf. Secur. Res.*, vol. 3, no. 1, pp. 236–245, Mar. 2013.

[17] A. Blum, B. Wardman, T. Solorio, and G. Warner, "Lexical feature based phishing URL detection using online learning," in *Proc. 3rd ACM Workshop Artif. Intell. Secur.*, Oct. 2010, pp. 54–60.

[18] M. Dunlop, S. Groat, and D. Shelly, "GoldPhish: Using images for content-based phishing analysis," in *Proc. 5th Int. Conf. Internet Monitor. Protection*, May 2010, pp. 123–128.

[19] J. Mao, W. Tian, P. Li, T. Wei, and Z. Liang, "Phishing-alarm: Robust and efficient phishing detection via page component similarity," *IEEE Access*, vol. 5, pp. 17020–17030, 2017.

[20] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: A content-based approach to detecting phishing web sites," in *Proc. 16th Int. Conf. World Wide Web*, May 2007, pp. 639–648.

[21] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep learning for phishing detection: Taxonomy, current challenges and future directions," *IEEE Access*, vol. 10, pp. 36429–36463, 2022.

[22] S. Maroofi, M. Korczyński, and A. Duda, "Are you human: Resilience of phishing detection to evasion techniques based on human verification," in *Proc. ACM Internet Meas. Conf.*, Oct. 2020, pp. 78–86.

[23] A. Oest, "PhishTime: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists," in *Proc. 29th USENIX Secur. Symp. (USENIX Secur.)*, 2020, pp. 379–396.

[24] K. Thomas, D. McCoy, C. Grier, A. Kolcz, and V. Paxson, "Trafcking fraudulent accounts: The role of the underground market in Twitter spam and abuse," in *Proc. 22nd USENIX Secur. Symp. (USENIX Secur.)*, 2013, pp. 195–210.

[25] S. Marchal, G. Armano, T. Gröndahl, K. Saari, N. Singh, and N. Asokan, "Off-the-hook: An efficient and usable client-side phishing prevention application," *IEEE Trans. Comput.*, vol. 66, no. 10, pp. 1717–1733, Oct. 2017.

[26] N. Samarasinghe and M. Mannan, "On cloaking behaviors of malicious websites," *Comput. Secur.*, vol. 101, Feb. 2021, Art. no. 102114.

[27] L. Invernizzi, K. Thomas, A. Kapravelos, O. Comanescu, J. Picod, and E. Bursztein, "Cloak of visibility: Detecting when machines browse a different web," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 743–758.

[28] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Inf. Syst.*, vol. 16, no. 4, pp. 527–565, Apr. 2022.

[29] P. Sharma, B. Dash, and M. F. Ansari, "Anti-phishing techniques—A review of cyber defense mechanisms," *IJARCCE*, vol. 11, no. 7, pp. 153–160, Jul. 2022.

[30] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, Jan. 2021.

[31] D. Xu, J. Pan, X. Du, B. Wang, M. Liu, and Q. Kang, "Massive fishing website URL parallel filtering method," *IEEE Access*, vol. 6, pp. 2378–2388, 2018.

[32] A. Oest, Y. Safei, A. Doupé, G. Ahn, B. Wardman, and G. Warner, "Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis," in *Proc. APWG Symp. Electron. Crime Res. (eCrime)*, May 2018, pp. 1–12.

[33] E. Merlo, M. Margier, G. Jourdan, and I. Onut, "Phishing kits source code similarity distribution: A case study," in *Proc. IEEE Int. Conf. Softw. Anal., Evol. Reeng. (SANER)*, Mar. 2022, pp. 983–994.

[34] G. V. Yudha and R. W. Wardhani, "Design of a snort-based IDS on the raspberry pi 3 model B+ applying TaZmen sniffer protocol and log alert integrity assurance with SHA-3," in *Proc. 9th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Aug. 2021, pp. 556–561, doi: 10.1109/ICoICT52021.2021.9527511.

[35] *King-Phisher*. Accessed: Apr. 8, 2023. [Online]. Available: https://www.kali.org/tools/

[36] sptoolkit. *Sptoolkit Rebirth Simple Phishing Toolki*. Accessed: Apr. 8, 2023. [Online]. Available: https://www.darknet.org.uk/2015/04/sptoolkit-rebirth-simple-phishing-toolkit/

[37] TrustedSec. *The Social-Engineer Toolkit (SET)*. Accessed: Apr. 8, 2023. [Online]. Available: https://www.trustedsec.com/tools/the-social-engineer-toolkitset/

[38] B. Kondracki, B. A. Azad, O. Starov, and N. Nikiforakis, "Catching transparent phish: Analyzing and detecting MITM phishing toolkits," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2021, pp. 36–50.

[39] J. Britt, B. Wardman, A. Sprague, and G. Warner, "Clustering potential phishing websites using DEEPMD5," in *Proc. 5th USENIX Workshop Large-Scale Exploits Emergent Threats, (LEET)*, 2012, pp. 1–8.

[40] Q. Cui, G.-V. Jourdan, G. V. Bochmann, R. Couturier, and I.-V. Onut, "Tracking phishing attacks over time," in *Proc. 26th Int. Conf. World Wide Web*, Apr. 2017, pp. 667–676.

[41] A. A. Orunsolu and A. S. Sodiya, "An anti-phishing kit scheme for secure web transactions," in *Proc. 3rd Int. Conf. Inf. Syst. Secur. Privacy*, 2017, p. 1524.

[42] F. Castaño, E. F. Fernañdez, R. Alaiz-Rodríguez, and E. Alegre, "PhiKitA: Phishing kit attacks dataset for phishing websites identification," *IEEE Access*, vol. 11, pp. 40779–40789, 2023.

[43] A. Karim, M. Shahroz, K. Mustofa, S. B. Belhaouari, and S. R. K. Joga, "Phishing detection system through hybrid machine learning based on URL," *IEEE Access*, vol. 11, pp. 36805–36822, 2023.

[44] H. Bijmans, T. Booij, A. Schwedersky, A. Nedgabat, and R. van Wegberg, "Catching phishers by their bait: Investigating the Dutch phishing landscape through phishing kit detection," in *Proc. 30th USENIX Secur. Symp. (USENIX Secur.)*, 2021, pp. 3757–3774.

[45] P. K. Sandhu and S. Singla, "Google safe browsing web security," *IJCSET*, vol. 5, no. 7, pp. 283–287, 2015.

[46] R. Verma and A. Das, "What's in a URL: Fast feature extraction and malicious URL detection," in *Proc. 3rd ACM Int. Workshop Secur. Privacy Anal.*, Mar. 2017, pp. 55–63.

[47] A. Basit, M. Zafar, A. R. Javed, and Z. Jalil, "A novel ensemble machine learning method to detect phishing attack," in *Proc. IEEE 23rd Int. Multitopic Conf. (INMIC)*, Nov. 2020, pp. 1–5.

[48] S. S. Roy, U. Karanjit, and S. Nilizadeh, "Evaluating the effectiveness of phishing reports on Twitter," in *Proc. APWG Symp. Electron. Crime Res. (eCrime)*, Dec. 2021, pp. 1–13.

[49] P. Peng, C. Xu, L. Quinn, H. Hu, B. Viswanath, and G. Wang, "What happens after you leak your password: Understanding credential sharing on phishing sites," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Jul. 2019, pp. 181–192.

[50] L. Tang and Q. H. Mahmoud, "A deep learning-based framework for phishing website detection," *IEEE Access*, vol. 10, pp. 1509–1521, 2022.

[51] L. R. Kalabarige, R. S. Rao, A. Abraham, and L. A. Gabralla, "Multilayer stacked ensemble learning model to detect phishing websites," *IEEE Access*, vol. 10, pp. 79543–79552, 2022.

[52] S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "Fame for sale: Efficient detection of fake Twitter followers," *Decis. Support Syst.*, vol. 80, pp. 56–71, Dec. 2015.

[53] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," *Expert Syst. Appl.*, vol. 41, no. 13, pp. 5948–5959, Oct. 2014.

[54] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, "PhishAri: Automatic realtime phishing detection on Twitter," in *Proc. eCrime Researchers Summit*, Oct. 2012, pp. 1–12.

[55] A. Oest, "Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale," in *Proc. 29th USENIX Secur. Symp. (USENIX Secur.)*, 2020, pp. 1–17.

[56] A. Oest, Y. Safaei, A. Doupé, G. Ahn, B. Wardman, and K. Tyers, "PhishFarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 1344–1361.

[57] M. Bitaab, H. Cho, A. Oest, P. Zhang, Z. Sun, R. Pourmohamad, D. Kim, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupe, and G.-J. Ahn, "Scam pandemic: How attackers exploit public fear through phishing," in *Proc. APWG Symp. Electron. Crime Res. (eCrime)*, Nov. 2020, pp. 1–10.

[58] B. Acharya and P. Vadrevu, "PhishPrint: Evading phishing detection crawlers by prior profiling," in *Proc. 30th USENIX Secur. Symp. (USENIX Secur.)*, 2021, pp. 3775–3792.

[59] R. Duan, W. Wang, and W. Lee, "Cloaker catcher: A client-based cloaking detection system," 2017, *arXiv:1710.01387*.

[60] P. Zhang, A. Oest, H. Cho, Z. Sun, R. Johnson, B. Wardman, S. Sarker, A. Kapravelos, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupé, and G. Ahn, "CrawlPhish: Large-scale analysis of client-side cloaking techniques in phishing," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 1109–1124.

[61] P. Zhang, Z. Sun, S. Kyung, H. W. Behrens, Z. L. Basque, H. Cho, A. Oest, R. Wang, T. Bao, Y. Shoshitaishvili, G.-J. Ahn, and A. Doupé, "I'm SPARTACUS, no. I'm SPARTACUS: Proactively protecting users from phishing by intentionally triggering cloaking behavior," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2022, pp. 3165–3179.

[62] P. Booth, S. A. Chaperon, J. S. Kennell, and A. M. Morrison, "Entrepreneurship in island contexts: A systematic review of the tourism and hospitality literature," *Int. J. Hospitality Manage.*, vol. 85, Feb. 2020, Art. no. 102438, doi: 10.1016/j.ijhm.2019.102438.

[63] M. A. Adebowale, K. T. Lwin, E. Sánchez, and M. A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of images, frames and text," *Expert Syst. Appl.*, vol. 115, pp. 300–313, Jan. 2019.

[64] M. Vijayalakshmi, S. Mercy Shalinie, M. H. Yang, and U. R. U. Meenakshi, "Web phishing detection techniques: A survey on the state-of-the-art, taxonomy and future directions," *IET Netw.*, vol. 9, no. 5, pp. 235–246, Sep. 2020.

[65] D. Kim, H. Cho, Y. Kwon, A. Doupé, S. Son, G.-J. Ahn, and T. Dumitras, "Security analysis on practices of certificate authorities in the HTTPS phishing ecosystem," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2021, pp. 407–420.

[66] B. Z. H. Zhao, M. Ikram, H. J. Asghar, M. A. Kaafar, A. Chaabane, and K. Thilakarathna, "A decade of mal-activity reporting: A retrospective analysis of Internet malicious activity blacklists," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Jul. 2019, pp. 193–205.

[67] S. Marchal, J. Franois, and T. Engel, "Proactive discovery of phishing related domain names," in *Proc. Int. Workshop Recent Adv. Intrusion Detection*. Cham, Switzerland: Springer, 2012, pp. 190–209.

[68] L.-H. Lee, K.-C. Lee, H.-H. Chen, and Y.-H. Tseng, "POSTER: Proactive blacklist update for anti-phishing," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 1448–1450.

[69] S. Marchal, J. François, R. State, and T. Engel, "PhishStorm: Detecting phishing with streaming analytics," *IEEE Trans. Netw. Service Manage.*, vol. 11, no. 4, pp. 458–471, Dec. 2014.

[70] N. Tsalis, N. Virvilis, A. Mylonas, T. Apostolopoulos, and D. Gritzalis, "Browser blacklists: The Utopia of phishing protection," in *Proc. Int. Conf. E-Bus. Telecommun.* Cham, Switzerland: Springer, 2014, pp. 278–293.

[71] S. Bell and P. Komisarczuk, "An analysis of phishing blacklists: Google safe browsing, OpenPhish, and PhishTank," in *Proc. Australas. Comput. Sci. Week Multiconference*, Feb. 2020, pp. 1–11.

[72] H. Shirazi, B. Bezawada, and I. Ray, "'*Kn0w Thy Doma1n Name*': Unbiased phishing detection using domain name based features," in *Proc. 23nd ACM Symp. Access Control Models Technol.*, Jun. 2018, pp. 69–75.

[73] R. S. Rao, T. Vaishnavi, and A. R. Pais, "CatchPhish: Detection of phishing websites by inspecting URLs," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 2, pp. 813–825, Feb. 2020.

[74] P. Peng, L. Yang, L. Song, and G. Wang, "Opening the blackbox of VirusTotal: Analyzing online phishing scan engines," in *Proc. Internet Meas. Conf.*, Oct. 2019, pp. 478–485.

[75] Y. Lin, "Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages," in *Proc. 30th USENIX Secur. Symp. (USENIX Secur.)*, 2021, pp. 3793–3810.

[76] S. Abdelnabi, K. Krombholz, and M. Fritz, "VisualPhishNet: Zero-day phishing website detection by visual similarity," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2020, pp. 1681–1698.

[77] B. Acharya and P. Vadrevu, "A human in every APE: Delineating and evaluating the human analysis systems of anti-phishing entities," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*. Cham, Switzerland: Springer, 2022, pp. 156–177.
[78] Y. Shin, K. Kim, J. J. Lee, and K. Lee, "Focusing on the weakest link: A similarity analysis on phishing campaigns based on the ATT&CK matrix," *Secur. Commun. Netw.*, vol. 2022, pp. 1–12, Apr. 2022.
[79] D. Patil, T. Pattewar, S. Pardeshi, V. Punjabi, and R. Wagh, "Learning to detect phishing web pages using lexical and string complexity analysis," *EAI Endorsed Trans. Scalable Inf. Syst.*, vol. 22, no. 1, p. e69, 2022.
[80] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Gone quishing: A field study of phishing with malicious QR codes," 2022, *arXiv:2204.04086*.
[81] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar, and S. Shukla, "Applications of deep learning for phishing detection: A systematic literature review," *Knowl. Inf. Syst.*, vol. 64, no. 6, pp. 1457–1500, Jun. 2022, doi: 10.1007/s10115-022-01672-x.

WENHAO LI (Graduate Student Member, IEEE) received the Bachelor of Engineering degree in information security from the Chengdu University of Information Technology, China, in 2019, the Master of Computer Science degree in cybersecurity from Arizona State University, and the M.B.A. degree from Webster University, USA, in 2022. He is currently pursuing the Ph.D. degree in cybersecurity with the National Advanced IPv6 Centre, Universiti Sains Malaysia. He is also the CEO of Chengdu Meetsec Technology Company Ltd., where he has successfully led many cybersecurity services, projects, and developments. His current research interests include wide range of cybersecurity topics, including anti-phishing, web security and privacy, cloud security, and the IoT security.

SELVAKUMAR MANICKAM is currently the Director of the National Advanced IPv6 Centre and an associate professor specializing in cybersecurity, the Internet of Things, industry 4.0, cloud computing, big data, and machine learning. He has authored or coauthored more than 220 articles in journals, conference proceedings, and book reviews. He has graduated 18 Ph.D. students in addition to master's and bachelor's students. He has given several keynote speeches and dozens of invited lectures and workshops at conferences, international universities, and industry. He has given talks and training on internet security, the Internet of Things, industry 4.0, IPv6, machine learning, software development, and embedded and OS kernel technologies at various organizations and seminars. He also lectures in various computer science and IT courses, including developing new courseware in tandem with current technology trends. He is involved in various organizations and forums locally and globally. Previously, he was with Intel Corporation and a few start-ups working in related areas before moving to academia. While building his profile academically, he is still very involved in industrial projects involving industrial communication protocol, robotic process automation, machine learning, and data analytics using opensource platforms. He also has experience in the building IoT, embedded, server, mobile, and web-based applications.

SHAMS UL ARFEEN LAGHARI received the B.Sc. (Hons.) and M.Sc. degrees in computer science from the University of Sindh, Jamshoro, Pakistan, and the M.S. degree in computer science from PAF-KIET, Karachi, Pakistan. He is currently pursuing the Ph.D. degree in network security with the National Advanced IPv6 Centre, Universiti Sains Malaysia. His research interests include cybersecurity, industry 4.0, distributed systems, cloud computing, and mobile cloud computing.

YUNG-WEY CHONG is currently a Senior Lecturer with the National Advanced IPv6 Centre, Universiti Sains Malaysia, where she has been a Faculty Member, since 2012. She worked in telecommunication industry before joining USM. Her research interests include industry revolution 4.0, ranging from embedded systems, wireless communication, cloud computing, and artificial intelligence. She has been involved in many collaborative research projects financed by various instances, including the European Commission, the Royal Academy of Engineering (U.K.), and the National Information Communication Technology (Japan).